In the Claims: (strikethrough parts deleted and underlined parts added)

Please cancel Claim 9 without prejudice.

1. (Currently Amended) A method of client account access protection for client/server or brick and mortar based transactions comprising:

storing ~~client~~ account holder defined access parameters input by an account holder ~~a client~~, wherein said ~~client~~ account holder defined access parameters define parameters that must be satisfied before a transaction of funds or information is authorized, wherein said account holder defined access parameters are stored on a server computer and wherein said account holder defined access parameters include geographic location parameters where said transaction is allowed to occur;

initiating a transaction of funds or information;

requesting account holder private information;

entering said account holder private information;

gathering other gathered information, where said other gathered information comprises the location of said entering said account holder private information for said transaction;

comparing said account holder private information along with said other gathered information with said ~~client~~ account holder defined access parameters; and

determining to authorize or deny said transaction based upon the results of said step of comparing.

2. (Currently Amended) A method according to claim 1 where said ~~client~~ account holder defined access parameters is any one or combination comprised of:

a password;

~~client~~ account holder accounts selected enabled or denied by ~~the client~~ said account holder for said transaction;

merchants selected enabled or denied for transaction with ~~client~~ said account holder accounts by ~~the client~~ said account holder;

~~geographic location parameters selected for association with a client account and merchants by the client where said transaction is allowed to occur;~~

a monetary amount associated with each account and merchant to limit the total amount of a single or a selected number of subsequent transactions;

a selection by ~~the client~~ said account holder to enable or deny access to ~~the client~~ said account holder accounts transacted through a bricks and mortar establishment and/or a network connection.

3. (Original) A method according to claim 2 where said geographic location parameters comprise Post Office zip codes, telephone area codes and telephone country codes.

4. (Original) A method according to claim 2 where said network comprises the Internet or Intranet.

5. (Currently Amended) A method according to claim 1 where said storing ~~client~~ account holder defined access parameters comprises storing ~~the~~ account holder defined access parameters on a secure network server accessed by ~~the client~~ a computing device.

6. (Currently Amended) A method according to claim 5 where ~~the client~~ said computing device comprises a personal computer, a workstation, an Automatic Teller Machine and a personal digital assistant.

7. (Currently Amended) A method according to claim 1 ~~where said~~ including establishing a connection ~~comprises~~ comprising the SET, TLS or SSL secure transaction protocol.

8. (Previously Amended) A method according to claim 1 where said requested account holder private information comprises name, address, password, account number or credit card number.

9. (Canceled)

10. (Currently Amended) A method according to claim 1 where said determining to authorize or deny the transaction comprises:

authorizing said transaction if requested private ~~client~~ account holder information and said other gathered information matches said ~~client~~ account holder defined access parameters; and

denying said transaction if the requested private ~~client~~ account holder information and said other gathered information does not match ~~the~~ said ~~client~~ account holder defined access parameters.

11. (Currently Amended) A method according to claim 1 including the step of changing said ~~client~~ account holder defined access parameters.

Please add the following claims:

12. (New) A method of client account access protection for client/server or brick and mortar based transactions comprising:

storing account holder defined access parameters input by an account holder, wherein said account holder defined access parameters define parameters that must be satisfied before a transaction of funds or information is authorized, wherein said account holder defined access parameters are stored on a server computer;

wherein said account holder defined access parameters include geographic location parameters where said transaction is allowed to occur;

where said geographic location parameters comprise Post Office zip codes, telephone area codes and telephone country codes;

initiating a transaction of funds or information;

requesting account holder private information;

entering said account holder private information;

gathering other gathered information, where said other gathered information comprises the location of said entering said account holder private information for said transaction;

comparing said account holder private information along with said other gathered information with said account holder defined access parameters; and

determining to authorize or deny said transaction based upon the results of said step of comparing.

13. (New) A method according to claim 12 where said account holder defined access parameters is any one or combination comprised of:

a password;

account holder accounts selected enabled or denied by said account holder for said transaction;

merchants selected enabled or denied for transaction with said account holder accounts by said account holder;

a monetary amount associated with each account and merchant to limit the total amount of a single or a selected number of subsequent transactions;

a selection by said account holder to enable or deny access to said account holder accounts transacted through a bricks and mortar establishment and/or a network connection.

14. (New) A method according to claim 12 where said network comprises the Internet or Intranet.

15. (New) A method according to claim 12 where said storing account holder defined access parameters comprises storing account holder defined access parameters on a secure network server accessed by a computing device.

16. (New) A method according to claim 15 where said computing device comprises a personal computer, a workstation, an Automatic Teller Machine and a personal digital assistant.

17. (New) A method according to claim 12 including establishing a connection comprising the SET, TLS or SSL secure transaction protocol.

18. (New) A method according to claim 12 where said requested account holder private information comprises name, address, password, account number or credit card number.

19. (New) A method according to claim 12 where said determining to authorize or deny the transaction comprises:

authorizing said transaction if requested private account holder information and said other gathered information matches said account holder defined access parameters; and

denying said transaction if the requested private account holder information and said other gathered information does not match said account holder defined access parameters.

20. (New) A method according to claim 12 including the step of changing said account holder defined access parameters.

21. (New) A method of client account access protection for client/server or brick and mortar based transactions comprising:

storing account holder defined access parameters input by an account holder, wherein said account holder defined access parameters define parameters that must be satisfied before a transaction of funds or information is authorized, wherein said account holder defined access parameters are stored on a server computer;

wherein said account holder defined access parameters include geographic location parameters where said transaction is allowed to occur, a password, account holder accounts selected enabled or denied by said account holder for said transaction, merchants selected enabled or denied for transaction with said account holder accounts by said account holder, a monetary amount associated with each account and merchant to limit the total amount of a single or a selected number of subsequent transactions, and a selection by said account holder to enable or deny access to said account holder accounts transacted through a bricks and mortar establishment and/or a network connection;

where said geographic location parameters comprise Post Office zip codes, telephone area codes and telephone country codes;

initiating a transaction of funds or information;

requesting account holder private information;

entering said account holder private information;

gathering other gathered information, where said other gathered information comprises the location of said entering said account holder private information for said transaction;

comparing said account holder private information along with said other gathered information with said account holder defined access parameters; and

determining to authorize or deny said transaction based upon the results of said step of comparing;

where said network comprises the Internet or Intranet; and

where said storing account holder defined access parameters comprises storing account holder defined access parameters on a secure network server accessed by a computing device.